

PREMIER MINISTRE

SECRÉTARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

DIRECTION CENTRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Schéma Français
d'Évaluation et de Certification
de la Sécurité des Technologies de l'Information

Rapport de certification 2001/12

Firewall M>Wall 4.0
sur BSD/OS version 3.1

Avril 2001

Ce document constitue le rapport de certification du produit “Firewall M>Wall 4.0 sur BSD/OS version 3.1”.

Ce rapport de certification est disponible sur le site internet de la Direction Centrale de la Sécurité des Systèmes d'Information à l'adresse suivante :

www.ssi.gouv.fr

Toute correspondance relative à ce rapport de certification doit être adressée au :

Secrétariat général de la Défense nationale
DCSSI
Centre de Certification
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.

Mél: certification.dcssi@sgdn.pm.gouv.fr

Ce document est folioté de 1 à 24 et certificat.



PREMIER MINISTRE

Schéma Français d'Évaluation et de Certification de la Sécurité des Technologies de l'Information

CERTIFICAT 2001/12

Firewall M>Wall 4.0 sur BSD/OS version 3.1

Développeur : MATRAnet

Commanditaire : MATRAnet

Les caractéristiques de sécurité du produit ci-dessus identifiées dans le rapport de certification ont été évaluées par un Centre d'Évaluation de la Sécurité des Technologies de l'Information selon les critères ITSEC.
Le niveau d'évaluation atteint est le **niveau E3**. La résistance minimum des mécanismes est cotée **moyenne**.
Ce certificat est valide pour la version du produit mentionnée, sous réserve du respect des recommandations d'utilisation et des restrictions éventuelles figurant dans le rapport de certification associé.

Le 18 mai 2001,

Le Commanditaire :
Le Président Directeur Général de MATRAnet

Claude GOUMY

L'Organisme de certification :
Le Directeur chargé de la sécurité des systèmes d'information
Henri SERRES

La présence du logo propre à l'Accord de Reconnaissance Mutuelle :

- *confirme que ce certificat a été délivré sous l'autorité d'un organisme de certification qualifié qui fait partie du Groupe d'Accord,*
- *indique que l'autorité de délivrance déclare qu'il s'agit d'un "certificat conforme" comme défini dans l'Accord,*
- *établit par conséquent des éléments pour baser la confiance dans le fait que le certificat est un "certificat conforme", bien que ne pouvant en donner une garantie, et qu'il sera reconnu en pratique par les autres membres du Groupe d'Accord.*

Les jugements contenus dans le certificat et le rapport de certification sont ceux de l'organisme de certification qualifié qui a procédé à la délivrance et ceux du centre d'évaluation de la sécurité des technologies de l'information qui a conduit l'évaluation. L'utilisation du logo de cet Accord n'entraîne pas la reconnaissance par les autres membres d'une quelconque responsabilité relative à ces jugements ou à tout dommage encouru en raison de la confiance accordée à ces jugements par une tierce partie.

Organisme de certification :
Secrétariat général de la Défense nationale
DCSSI
51, boulevard de Latour-Maubourg
75700 PARIS 07 SP.



Chapitre 1

Introduction

1 Ce document représente le rapport de certification du produit “Firewall M>Wall 4.0 sur BSD/OS version 3.1” développé par MATRAnet.

2 Le produit M>Wall est un logiciel garde-barrière conçu pour contrôler les communications entre un réseau externe et un réseau privé interne à protéger.

3 La cible d’évaluation est constituée du filtre de paquets IP, d’un ensemble de relais applicatifs pour les protocoles Internet les plus courants (SMTP, HTTP) ou critiques du point de vue de la sécurité (RLOGIN et TELNET), d’un relais générique pour les autres applications de TCP, de fonctionnalités de contrôle d’accès par adresse ainsi que d’un mécanisme de contrôle d’intégrité de sa propre configuration.

4 Les fonctions dédiées à la sécurité évaluées sont décrites dans le chapitre 4 du présent rapport.

5 Le produit M>Wall 4.0 sur BSD/OS version 3.1 dont les fonctions dédiées à la sécurité évaluées sont décrites dans le chapitre 4 du présent rapport, satisfait aux exigences du niveau d’évaluation ITSEC E3/moyen.

Chapitre 2

Résumé

2.1 Conclusions de l'évaluation

6 La cible d'évaluation détaillée au chapitre 3 du présent rapport satisfait aux exigences du **niveau d'évaluation E3**.

7 La résistance minimale des mécanismes de sécurité de la cible d'évaluation est cotée **moyenne**.

8 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau E3 et par la compétence, l'opportunité et les ressources correspondant à la cotation moyenne de la résistance minimum des mécanismes.

9 Les fonctions de sécurité qui ont été évaluées sont définies au chapitre 4 du présent rapport.

10 Les vulnérabilités connues du commanditaire de l'évaluation ont toutes été communiquées à l'évaluateur et au certificateur conformément aux critères [ITSEC 3.26] et [ITSEC 3.35].

11 L'utilisation sécuritaire de la cible d'évaluation est soumise aux recommandations figurant dans le chapitre 5 du présent rapport.

2.2 Contexte de l'évaluation

12 L'évaluation a été menée conformément aux critères ITSEC [ITSEC], à la méthodologie définie dans le manuel ITSEM [ITSEM] et aux interprétations définies dans la bibliothèque d'interprétation commune JIL [JIL].

13 L'évaluation s'est déroulée consécutivement au développement du produit.

14 La cible d'évaluation a été développée par la société MATRAnet :

- MATRAnet
  18 rue Grange Dame Rose
  BP 262
  78147 Vélizy Cedex
  France

Le développeur de la cible d'évaluation est aussi le commanditaire de l'évaluation.

15 Cette évaluation a été conduite par le Centre d'Evaluation de la Sécurité des Technologies de l'Information de la société AQL (ci-après "l'évaluateur") :

- AQL
  rue de la Châtaigneraie
  BP 127
  35513 Cesson-Sévigné Cedex
  France

Chapitre 3

Identification de la cible d’évaluation

3.1 Objet

16 M>Wall permet la mise en oeuvre d’une politique de sécurité régissant les échanges entre un réseau interne à protéger et un réseau externe. Il fournit un ensemble de filtres ou relais applicatifs qui opèrent un contrôle des flux d’informations qui le traversent, contrôlent les protocoles utilisés, contrôlent la syntaxe des commandes applicatives transmise, et authentifient les utilisateurs distants à l’aide de mots de passe à usage unique.

17 Dans la configuration évaluée, M>Wall est installé en coupure entre le réseau interne à protéger et le réseau externe. La configuration à trois réseaux est exclue de l’évaluation.

18 L’administration du firewall est réalisée à l’aide d’un outil permettant de se connecter directement au système d’exploitation. L’administration à distance ne fait pas partie de la cible d’évaluation.

3.2 Historique du développement

19 Le produit a été développé par la société MATRAnet sur son site de Vélizy.

3.3 Description des matériels

20 La cible d’évaluation ne comporte pas d’élément matériel. Les composants logiciels de la cible nécessitent cependant une configuration matérielle minimale pour assurer un fonctionnement correct.

21 La configuration de test utilisée pour l’évaluation est un PC Intel Pentium équipé des élements suivants :

- 128 Mo de RAM ;
- un disque dur IDE de 8 Go ;
- deux cartes réseaux Ethernet 3C509.

3.4 Description des logiciels

22 Les composants logiciels de M>Wall s’appuient sur le système d’exploitation BSD/OS version 3.1. Le système d’exploitation BSD/OS version 3.1 est la version modifiée par MATRAnet du système BSD/OS version 3.0. Cette mise-à-niveau de

la version 3.0 doit être exécutée durant l’installation de M>Wall expliquée dans le guide d’installation [INSTALL].

23 La cible d’évaluation est composée des éléments logiciels suivants :

- filtre dynamique des paquets IP ;
- `netacl` contrôlant l’accès aux services et relais applicatifs du produit ;
- relai applicatif `plug_gw` pour les protocoles webster, whois, NNTP, qotd et autres services TCP ;
- relai applicatif `http_gw` pour les protocoles HTTP, SHTTP, SSL, FTP en mode passif, Gopher ;
- relai applicatif `rlogin_gw` pour le protocole rlogin ;
- relai applicatif `telnet_gw` pour le protocole TELNET ;
- `smap/smapd` pour la transmission des messages SMTP ;
- administration locale ;
- calcul de condensats MD5 ;
- authentification des utilisateurs basée sur S/Key et MD5.

24 Le noyau 4.4BSD du système d’exploitation BSD/OS 3.1 fait également partie de la cible d’évaluation.

3.5 Description de la documentation

25 La documentation du produit est constituée :

a) d’un manuel pour les utilisateurs de l’authentification [UTIL],

b) d’un manuel d’installation [INSTALL],

c) d’un manuel d’administration [ADMIN],

d) d’une cible de sécurite [ST].

Chapitre 4

Caractéristiques de sécurité

4.1 Préambule

26 Les fonctions ou mécanismes de sécurité évaluées sont décrits dans la cible de sécurité [ST] qui est la référence pour l'évaluation. Les paragraphes ci-après reformulent les éléments essentiels de cette cible.

4.2 Hypothèses

27 Les résultats de l'évaluation sont conditionnés par le respect des hypothèses sur l'utilisation et l'environnement d'utilisation de la cible d'évaluation suivantes :

- Protections physiques :
  - le firewall doit être installé en coupure entre le réseau interne à protéger et le réseau externe,
  - l'accès physique au firewall doit être protégé et limité à l'administrateur. Seule l'administration locale est autorisée.
- Personnel :
  - l'administrateur doit être une personne de confiance.
- Organisation :
  - le firewall est destiné à n'être utilisé qu'en tant que firewall et ne doit pas fournir d'autres services aux utilisateurs des deux réseaux (interne et externe). Seul l'administrateur doit pouvoir se connecter directement au firewall,
  - des procédures de contrôle et d'archivage des données d'audit du firewall doivent être mises en place,
  - des procédures de contrôle régulier de la configuration du firewall doivent être mises en place pour s'assurer de l'adéquation de la configuration avec la politique de sécurité globale du réseau interne. De la même façon, l'intégrité des fichiers du firewall doit être vérifiée régulièrement,
  - les systèmes sur lesquels sont stockés les mots de passe jetables distribués aux utilisateurs doivent garantir la protection de ces mots de passe,
  - les condensats utilisés pour vérifier l'intégrité des fichiers du firewall doivent être stockés sur une machine séparée du firewall,
  - l'utilisation de "trusted host" pour le protocole rlogin doit être contrôlée et limitée,
  - l'administrateur doit modifier son mot de passe au moins une fois par mois et le choisir d'une taille supérieure à 7 caractères alphanumériques.

28 Le détail de ces hypothèses est disponible dans la cible de sécurité [ST].

4.3 Menaces

29 Les menaces couvertes par la cible d'évaluation sont celles qui sont définies dans la cible de sécurité [ST]. Elles peuvent être résumées comme suit :

- utilisation illicite d'un service du réseau interne par un utilisateur externe,
- fourniture illicite d'un service réservé au réseau interne par un utilisateur externe ;
- fourniture illicite d'un service interdit dans le réseau interne par un utilisateur externe ;
- utilisation d'un service interne autorisé aux utilisateurs externes afin d'accéder à d'autres services interdits ;
- accès illicite au firewall ;
- introduction d'applets Java malicieuses dans le réseau interne par le biais du service http ;
- transmission vers le réseau externe de requêtes à des services internes.

4.4 Fonctions dédiées à la sécurité de la cible d'évaluation

30 Les fonctions dédiées à la sécurité évaluées sont les suivantes :

a) Fonctions d'identification et d'authentification de l'administrateur

- L'administrateur doit s'authentifier auprès de BSD/OS avant de pouvoir administrer le firewall.
- L'administrateur ne peut pas se connecter à distance.

b) Fonctions de contrôle d'accès

- Certains paquets jugés dangereux (ceux portant une option IP "routage par la source", ceux usurpant une adresse interne) ou ne correspondant à aucune règle de filtrage ou n'ayant pas de processus destinataire légitime sont détruits, éventuellement en générant un enregistrement d'audit.
- Chaque paquet IP reçu sur une interface réseau fait l'objet d'un contrôle configurable portant sur les en-têtes protocolaires connus, à savoir IP, ICMP, UDP, TCP. La conclusion de ce contrôle détermine si le paquet est :
  - détruit (éventuellement en générant un enregistrement d'audit) ou
  - dirigé vers un programme applicatif (généralement un relai applicatif) ou
  - retransmis vers le réseau opposé à son réseau d'origine.
- Chaque connexion TCP peut être acceptée ou refusée en fonction de l'adresse du client et de la machine demandée. Les critères utilisés sont configurables.
- L'utilisation des services TELNET et RLOGIN peut être restreinte à une plage horaire arbitraire en fonction de l'utilisateur concerné.
- La cible d'évaluation filtre les références aux "applets" Java dans les pages HTML qui traversent le relai applicatif HTTP.

- La cible fournit la possibilité de calculer un condensat de tous les fichiers du firewall pour détecter leur modification.
- Certains relais applicatifs peuvent changer d'identité et se limiter à un sous arbre du système de fichiers pour se protéger d'interférences mutuelles.

c) Fonctions d'audit

- En plus des enregistrements référencés ci-dessus, chaque relais applicatif génère un enregistrement d'audit pour signaler :
  - le début et la fin de chaque connexion TCP,
  - les fichiers critiques inexistants et un sous-ensemble des erreurs de syntaxe dans la configuration.
  - l'utilisation du mécanisme d'authentification
  - une incohérence entre le nom de machine et l'adresse IP pour tout client d'un relai applicatif ou destination demandée à un relai applicatif.
- La cible fournit des outils configurables pour résumer son activité.
- Un enregistrement d'audit contient un sous ensemble des éléments suivant selon leur pertinence :
  - date, heure et type de l'évènement
  - adresse IP et nom pleinement qualifié (source et destination pour les paquets, client et serveur pour les connexions)
  - commandes individuelles pour le relai applicatif HTTP

d) Fonctions d'authentification des utilisateurs

- Les utilisateurs qui veulent utiliser RLOGIN ou TELNET doivent être authentifiés par S/Key.
- Les données d'authentification ne sont jamais transmises sur un réseau, même interne.

31 Le détail de ces fonctions est disponible dans la cible de sécurité [ST].

Chapitre 5

Résultats de l'évaluation

5.1 Rapport Technique d'Évaluation

50 Les résultats de l'évaluation sont exposés dans le Rapport Technique d'Evaluation [RTE].

5.2 Principaux résultats de l'évaluation

51 Le produit répond aux exigences des critères ITSEC pour le niveau E3.

5.2.1 Exigences de conformité

Spécifications des besoins

52 Les critères ITSEC pour cette phase de la conformité sont définis dans les paragraphes E3.2, E3.3 et E3.4 du document ITSEC.

53 La cible de sécurité rédigée par le commanditaire décrit l'ensemble des fonctions dédiées à la sécurité. L'argumentaire du produit précise l'environnement d'utilisation prévu ainsi que le mode d'utilisation prévu. Les objectifs de sécurité sont précisés. Une correspondance est établie entre les fonctions dédiées à la sécurité et les menaces.

54 Le document cible de sécurité [ST] précise comment les fonctions dédiées à la sécurité sont appropriées aux modes d'utilisation prévus et adéquates pour contrer les menaces supposées. L'évaluateur s'est assuré de l'absence d'incohérence dans la cible de sécurité.

Conception générale

55 Les critères ITSEC pour cette phase de la conformité sont définis dans les paragraphes E3.5, E3.6 et E3.7 du document ITSEC.

56 Le développeur a fourni la description de la structure générale du produit, ainsi que de l'ensemble des composants logiciels.

57 Le document fourni identifie également les interfaces externes de la cible d'évaluation. Ces interfaces sont de trois types :

- interfaces avec le "terminal management" permettant d'administrer localement le firewall,
- interfaces réseau,
- interfaces logiques.

Conception détaillée

58 Les critères ITSEC pour cette phase de la conformité sont définis dans les paragraphes E3.8, E3.9 et E3.10 du document ITSEC.

59 Le développeur a fourni la conception des composants élémentaires qui mettent en oeuvre les composants principaux issus de la conception générale. La spécification ainsi que les interfaces de ces composants élémentaires y sont décrites.

60 Les spécifications des mécanismes de sécurité qui réalisent l'ensemble des fonctions dédiées à la sécurité ont également été fournies.

61 L'évaluateur a analysé la manière dont ces mécanismes assurent les fonctions de la cible d'évaluation et s'est assuré de la traçabilité pertinente entre les fonctions dédiées à la sécurité, les composants et les mécanismes de sécurité.

Réalisation

62 Les critères ITSEC pour cette phase de la conformité sont définis dans les paragraphes E3.11, E3.12 et E3.13 du document ITSEC.

63 Le code source des mécanismes réalisant les fonctions dédiées à la sécurité a été fourni à l'évaluateur. Celui-ci a ainsi pu vérifier que ces mécanismes ont été correctement implémentés.

64 Par ailleurs, cette analyse détaillée du code source a permis à l'évaluateur de détecter d'éventuelles vulnérabilités potentielles.

65 La documentation de tests décrivant le plan des tests, l'objectif des tests et les procédures de tests à réaliser a été fournie à l'évaluateur.

66 L'évaluateur a procédé sur sa plate-forme de test au rejeu de l'intégralité des programmes de tests livrés par le développeur.

67 L'évaluateur a procédé à une analyse indépendante pour vérifier que les tests couvrent bien toutes les fonctions dédiées à la sécurité. La couverture du code source par les tests a été vérifiée sur l'ensemble du code source dédié à la sécurité.

Gestion de configuration

68 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.15, E3.16 et E3.17 du document ITSEC.

69 Le développeur utilise un système de gestion de configuration basé sur l'outil CVS.

70 A chaque étape du cycle de vie du produit, les objets produits sont mis sous contrôle du système de gestion de configuration conformément à une procédure bien définie.

71 La liste de configuration donnée par le développeur identifie les fichiers sources ainsi que les documents de développement.

72 L’utilisation effective du système de gestion de configuration mis en place sur le site de Vélizy a pu être vérifiée par l’évaluateur lors des visites de mai et de septembre 2000.

Langages de programmation

73 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.18, E3.19 et E3.20 du document ITSEC.

74 Les langages utilisés pour la réalisation du code source sont : le langage C, Perl version 5 et le "Bourne shell". Les langages sont correctement définis et accompagnés des documents de référence.

75 L’évaluateur a vérifié lors de l’inspection du code source que toutes les instructions utilisées sont documentées dans ces manuels de référence.

Sécurité des développeurs

76 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.21, E3.22 et E3.23 du document ITSEC.

77 L’évaluateur a analysé la sécurité du développement chez MATRAnet.

78 Des procédures physiques, organisationnelles, techniques, liées au personnel assurent un niveau de protection suffisant de la cible d'évaluation, de ses constituants ainsi que de sa documentation.

79 Deux visites du site de développement de Vélizy en juin 1999 et mai 2000 ont permis de vérifier l'application de ces procédures.

Documentation utilisateur et d’administration

80 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.25, E3.26 et E3.27 ainsi que E3.28, E3.29, E3.30 du document ITSEC.

81 La seule fonction de sécurité qui concerne directement l’utilisateur final est son authentification lors de l’utilisation d’un service relayé par le firewall. Le manuel pour les utilisateurs de l’authentification [UTIL] décrit la méthode d’authentification et les précautions à prendre pour protéger les données d’authentification, ici les mots de passe à usage unique et le germe.

82 La documentation d’administration est constituée des manuels d’administration [ADMIN] et d’installation [INSTALL].

83 Le manuel d’administration décrit notamment les points suivants :

- les paramètres de configuration du filtre de paquets, des relais applicatifs, la gestion des comptes utilisateurs ;

- le suivi au quotidien de la sécurité, via les journaux d’audit, notamment la génération et la personnalisation des rapports d’activité du firewall ;
- l’utilisation des analyseurs syntaxiques qui vérifient que la configuration du firewall est valide avant sa mise en service.

Livraison et configuration

84 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.32, E3.33 et E3.34 du document ITSEC.

85 Le produit M>Wall est disponible dans différentes versions (relatives à différents systèmes d'exploitation) mais la cible d'évaluation ne correspond qu'à une seule de ces versions : la version s'exécutant sur BSD/OS version 3.1. Il n'existe donc qu'une seule configuration possible de la cible d'évaluation et cette configuration évaluée est définie de façon satisfaisante dans la cible de sécurité [ST].

86 Les procédures d’installation sont décrites dans le manuel d’installation [INSTALL]. Ces procédures comprennent :

- l'installation de BSD/OS (chapitre 1.5),
- l'installation de BSD/OS - phase 2 (chapitre 1.6),
- l'installation de BSD/OS - phase 3 (chapitre 1.7),
- l'installation du firewall (chapitre 1.8).

87 La procédure de livraison consiste à transmettre la cible en deux parties séparées :

a) un colis contenant le CDROM version 3.1 de BSD/OS, le CDROM version 4.0 du M>Wall certifiée, la disquette de boot pour l'installation de BSD/OS, les documentations d'installation et d'exploitation [UTIL], [ADMIN] et [INSTALL],

b) un colis contenant une disquette sur laquelle se trouvent la licence de la cible d'évaluation et la signature MD5 des fichiers contenus sur le CDROM "M>Wall certifié".

88 Les deux colis sont ensuite envoyés par des canaux de communication différents (par la poste et par un porteur ou par la poste uniquement mais avec quelques jours d'intervalle).

Démarrage et exploitation

89 Les critères ITSEC pour cet aspect de la conformité sont définis dans les paragraphes E3.35, E3.36 et E3.37 du document ITSEC.

90 La documentation de démarrage et d’exploitation est intégrée à la documentation d’administration du produit [ADMIN]. Ce manuel fournit en complément un exemple de journal d’audit généré au cours de l’exploitation du produit.

5.2.2 Exigences en efficacité

Pertinence

91 Les critères ITSEC pour cet aspect de l’efficacité sont définis dans les paragraphes 3.14, 3.15 et 3.16 du document ITSEC.

92 L'analyse de pertinence a été faite à deux niveaux : une analyse de pertinence des fonctions qui montre comment les menaces sont contrées par les fonctions dédiées à la sécurité et une analyse de pertinence des mécanismes dédiés à la sécurité qui montre comment les menaces sont contrées par ces mécanismes.

93 Les analyses de pertinence du développeur s'appuient sur la conception détaillée de la cible d'évaluation.

Cohésion

94 Les critères ITSEC pour cet aspect de l’efficacité sont définis dans les paragraphes 3.18, 3.19 et 3.20 du document ITSEC.

95 L'analyse de cohésion a également été faite à deux niveaux : une analyse de cohésion des fonctions qui montre qu'aucune interaction entre deux fonctions dédiées à la sécurité ne crée de faiblesse pour la sécurité ; puis une analyse de cohésion des mécanismes dédiés à la sécurité qui montre que les mécanismes dédiés à la sécurité coopèrent pour former un ensemble intégré et efficace.

96 Les analyses de cohésion du développeur ont pris en compte la conception détaillée de la cible d'évaluation.

Résistance des mécanismes

97 Les critères ITSEC pour cet aspect de l’efficacité sont définis dans les paragraphes 3.22, 3.23 et 3.24 du document ITSEC.

98 Le développeur a rédigé une analyse de la résistance des mécanismes. La liste des mécanismes critiques de M>Wall a ainsi été établie.

99 L’évaluateur a analysé cette documentation et mené une cotation indépendante des mécanismes. Cette cotation est en accord avec l’analyse du développeur.

100 La résistance moyenne des mécanismes utilisant des calculs cryptographiques a été confirmée par la DCSSI sous réserve du respect des recommandations d’utilisation de la cible d’évaluation résumées au chapitre 6.

101 La cotation globale des mécanismes est considérée comme moyenne. Les tests de pénétration ont permis de confirmer cette cotation.

Facilité d'emploi

102 Les critères ITSEC pour cet aspect de l'efficacité sont définis dans les paragraphes 3.31, 3.32 et 3.33 du document ITSEC.

103 Le développeur a fourni une analyse de la facilité d'emploi de la cible d'évaluation avec la documentation d'exploitation disponible.

104 L'évaluateur a pu s'assurer que les états non sûrs dans lesquels peut transiter le produit sont soit détectés par le logiciel (les relais applicatifs ou les analyseurs syntaxiques) soit décrits dans la documentation d'administration pour prévenir l'administrateur des conséquences de ses actes.

Vulnérabilités de la construction et en exploitation

105 Les critères ITSEC pour ces aspects de l'efficacité sont définis dans les paragraphes 3.26, 3.27, 3.28 et 3.35, 3.36, 3.37 du document ITSEC.

106 L'analyse de vulnérabilités a été menée en connaissance de toutes les informations fournies à l'évaluateur pour le niveau E3.

107 L'évaluateur s'est assuré à travers des tests de pénétration que les vulnérabilités potentielles en construction et en exploitation ne sont pas exploitables même avec un niveau moyen de ressource de l'attaquant tel que défini par la cotation de la résistance des mécanismes.

Verdicts

108 Pour tous les aspects des critères ITSEC identifiés ci-dessus, un avis “réussite” a été émis.

Chapitre 6

Recommandations d’utilisation

109 La cible d’évaluation “Firewall M>Wall 4.0 sur BSD/OS version 3.1” est soumise aux recommandations d’utilisation exprimées ci-dessous. Le respect de ces recommandations conditionne la validité du certificat.

a) Le produit doit être utilisé conformément à l’environnement d’utilisation prévu dans la cible de sécurité [ST]. Les hypothèses pour l’évaluation portent notamment sur les points suivants :

- le firewall doit être installé en coupure entre le réseau interne à protéger et le réseau externe,
- l’accès physique au firewall doit être protégé et limité à l’administrateur. Seule l’administration locale est autorisée,
- le firewall est destiné à n’être utilisé qu’en tant que firewall et ne doit pas fournir d’autres services aux utilisateurs des deux réseaux (interne et externe). Seul l’administrateur doit pouvoir se connecter directement au firewall,
- des procédures de contrôle régulier des journaux d’audit et de la configuration du firewall doivent être mises en place.

b) l’authentification des utilisateurs des services rlogin et telnet doit impérativement utiliser S/Key avec MD5 ; le germe utilisé pour générer les mots de passe doit contenir au moins 10 caractères alphanumériques ;

c) l’option permettant le changement de mot de passe à distance ne doit pas être activée ;

d) les analyseurs syntaxiques destinés à vérifier les fichiers de configuration doivent être utilisés ;

e) les applets Java doivent être interdites dès l’installation du produit et des mesures externes doivent être prises pour interdire l’entrée de texte HTML via une autre voie que le relai applicatif HTTP. Cela inclu en particulier le courrier électronique entrant.

Chapitre 7

Certification

Certification

7.1 Objet

110 Le produit M>Wall 4.0 sur BSD/OS version 3.1 dont les caractéristiques de sécurité sont définies dans le chapitre 4 du présent rapport, satisfait aux exigences du **niveau d'évaluation E3**.

111 La résistance minimum des mécanismes est cotée **moyenne.**

112 La recherche de vulnérabilités exploitables au cours de l'évaluation a été définie par la quantité d'informations disponibles pour le niveau E3 et par la compétence, l'opportunité et les ressources correspondant à la cotation moyenne de la résistance minimum des mécanismes.

7.2 Portée de la certification

113 La certification ne constitue pas en soi une recommandation du produit. Elle ne garantit pas que le produit certifié est totalement exempt de vulnérabilités exploitables : il existe une probabilité résiduelle (d'autant plus faible que le niveau d'évaluation est élevé) que des vulnérabilités exploitables n'aient pas été découvertes.

114 Le certificat ne s'applique qu'à la version évaluée du produit.

115 La certification de toute version ultérieure nécessitera au préalable une réévaluation en fonction des modifications apportées.

Annexe A

Glossaire

Biens	Informations ou ressources à protéger par la cible d'évaluation ou son environnement.
Cible d'évaluation	Un produit ou un système et la documentation associée pour l'administrateur et pour l'utilisateur qui est l'objet d'une évaluation.
Cible de sécurité	Un ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation identifiée.
Evaluation	Estimation d'une cible d'évaluation par rapport à des critères définis.
FTP	File Transfer Protocol - Protocole utilisé pour le transfert de fichiers.
HTTP	HyperText Transfer Protocol - Protocole utilisé pour le transfert de pages web.
ICMP	Internet Control Message Protocol - Protocole utilisé pour la signalisation de cas d'erreur et le contrôle des opérations de la couche IP.
IP	Internet Protocol.
Proxy	Relai applicatif.
SMTP	Simple Mail Transfer Protocol - Protocole utilisé pour la transmission de messages électroniques.

Annexe B

Références

[ITSEC] Critères d'évaluation de la sécurité des systèmes informatiques, version 1.2, juin 1991.

[ITSEM] Manuel d'évaluation de la sécurité des technologies de l'information, version 1.0, septembre 1993.

[JIL] ITSEC Joint Interpretation Library, version 2.0, novembre 1998.

[ST] M>Wall 4.0 - Security Target, réf. 100-400-200003, version 1.7, 24 novembre 2000 (document public).

[RTE] Rapport Technique d'Evaluation, réf. MTN002-RTE01-1.00, version 1.00, 17 avril 2001 (diffusion contrôlée).

[UTIL] M>Wall 4.0 - Manuel pour les utilisateurs de l'authentification, réf. 501-400-200007, version 1.2.

[INSTALL] M>Wall 4.0 - Accompagnement d'installation, réf. 116-400-200003, version 2.4.

[ADMIN] M>Wall 4.0 - Manuel d'administration, réf. 500-400-200003, version 1.6.